



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,334	06/30/2003	Dario Bazan Bejarano	MFCP.102772	8771
45809 7590 11/23/2007 SHOOK, HARDY & BACON L.L.P. (c/o MICROSOFT CORPORATION) INTELLECTUAL PROPERTY DEPARTMENT 2555 GRAND BOULEVARD KANSAS CITY, MO 64108-2613			EXAMINER REZA, MOHAMMAD W	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 11/23/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/608,334	<b>Applicant(s)</b> BAZAN BEJARANO, DARIO	
	<b>Examiner</b> Mohammad W. Reza	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 12 September 2007.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-32 and 49-62 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-32, and 49-62 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. This is in response to the arguments filed on 09/12/2007.
2. Claims 1-32, and 49-62 are pending in the application.
3. Claims 1-32, and 49-62 have been rejected.

### *Response to Arguments*

4. Applicant's arguments filed on 07/27/2007 have been fully considered but they are not persuasive.

Applicant argues that Bathrick's reference does not disclose the limitations of the independent claims 1, 17, and 49. Specifically, applicant mentioned that Bathrick fails to teach, "Comparing a first protocol set associated with the internal node to a second protocol set associated with the external node, and establishing a secure connection between the external node and the internal node when a matching protocol between the first protocol set and second protocol set is found". According to the applicant's specification this limitations are described as, "According to the invention either of an external agent or an internal agent may initiate an attempt to establish a secure session across the domain boundary, transmitting a request including a set of supported protocols to the recipient machine. **A negotiation engine may then compare** the available protocols on both of the agents, nodes or machines at either end of the session, and

**select a compatible protocol when found.** The internal and external agents may likewise authenticate each other using a key, certificate or other mechanism (abstract)", and "According to the invention in one regard, a network manager or other agent or node within a security-enabled domain may initiate an attempt to establish a secure connection with an external agent or node. That request may contain a data field indicating a set of security protocols available for use by the manager. The external agent may receive the request and compare the protocols available to the internal agent or manager to a set of protocols supported by the external agent. If a match between available protocols is found, communications may proceed based on that selected protocol (paragraphs, 0007)". So it is understandable from the spec. that a **negotiation process** takes place between internal and external node through comparing the protocols belongs to them. Barhrick discloses this limitation. "In response to the data transfer request signal, the next step in the method is to **compare** the data unit address with the end-system addresses, security keys and **protocol specifications**. In **response to a match**, a transmit enable signal is generated.....Upon generation of the security key, a transfer enable signal is generated and a security protocol data transfer is performed. The security protocol processor 28 of end-system B receives the data unit

from end-system A and applies the appropriate security protocol when decoding data. The data unit is then passed to the end-system B user (col. 4, lines 37-54)". So the aforementioned citations shows that Bethrich teaches about two end systems compare their protocols and if the match is found then the connection establishes. Bethrich's SAS address is the correspondent of one of the security protocol specifications. It is clearly applicant's misinterpretation that Bethrich invention is only comparing the protocol address. The main idea of this invention is to compare the two different protocol sets through the negotiation process. Bethrich describes in details how this negotiation steps are performed and comparing the SAS address (which is one of the security protocol specifications) is part of that protocol comparison. It is not just address comparison between two end systems. So, by comparing the SAS address, Bethrich actually comparing the two protocols sets not anything else. For example, "The method of the sequence of steps described above in reference to FIG. 2 and comprises the steps of storing a set of end-system addresses and corresponding security keys and **security protocol specifications (SAS addresses)** and storing a set of addresses of end-systems that require a security protocol for data unit transmission (PAS addresses). In response to generation of a data unit, which includes **an end-system address and a corresponding required security protocol**, the method generates a data transfer request signal (col. 4, lines 26-36)". It is clear that the address (SAS address) is the represent of the security protocol of the end system not anything else. So, comparing the SAS

addresses of the corresponding protocols is actually comparing the security protocols, in deed. For example, "The invention includes processing means which, upon reception of a request for the transmission of a protocol data unit, automatically searches the "Secure Address Store" for an entry whose address matches the destination address of the protocol data unit. If an entry is found in the "Secure Address Store" with such an address, then the protocol data unit is automatically transmitted in accordance with the appropriate security protocol, and protected with the appropriate key (col. 2, lines 1-6)", "If a match is found in the "Protocol Address Store" the invention automatically invokes **the appropriate process negotiation** to obtain a key and **a determination of which security protocol to use** (col. 2, lines 14-17)", and "Upon receipt of the negotiation completion signal, further processing of the protocol data unit includes the application of the appropriate security protocol and **automatic transmission of the data unit**. (col. 2, lines 23-27)". These citation parts disclose the comparison and establishment of the connection if two protocols of the end systems are matched. All the dependent claims are rejected at least their dependency on the independent claims.

*Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-32, and 49-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bathrick et al hereafter Bathrick (US patent 5010572) in view of Marino, Jr. et al hereafter Marino (US Patent 5530758).
6. As per claim 1, Bathrick discloses a method for automatically negotiating a security protocol, comprising: comparing a first protocol set associated with the internal node to a second protocol set associated with the external node; and establishing a secure connection between the external node and the internal node when a matching protocol between the first protocol set and the second protocol set is found (abstract, col. 1, lines 53-67, col. 2, lines 1-32). Although, Bathrick discloses establishing a secure connection between two nodes based on protocol (abstract, col. 1, lines 53-67, col. 2, lines 1-32), he does not explicitly disclose receiving a security authorization request to establish a secure connection between an internal node, the internal node being internal to a security-enabled domain, and an external node, the external node being external to the security-enabled domain. Nevertheless, it is well known in the network security art at the time of invention that a security domain will authorize to establish a connection with

other nodes outside of that domain. Exemplary of this is Marino who discloses receiving a security authorization request to establish a secure connection between an internal node, the internal node being internal to a security-enabled domain, and an external node, the external node being external to the security-enabled domain (col. 3, lines 1-67, abstract).

Accordingly, it would been obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Marino's teachings of operational methods for a secure node in a computer network with the teachings of Bathrick, for the purpose of suitably establishing the connection between two nodes in accordance with their protocol matching (col. 3-4).

7. As per claim 2-5, Bathrick does not disclose a method wherein the external node comprises at least one of a computer and a network-enabled wireless device, wherein the internal node comprises at least one of a client computer and a server, wherein the security-enabled domain comprises a distributed directory domain, wherein the security-enabled domain comprises a certificate-based domain. However, Marino discloses wherein the external node comprises at least one of a computer and a network-enabled wireless device (col. 4, lines 26-67), wherein the internal node comprises at least one of a client computer and a server, wherein the security-enabled domain comprises a distributed directory domain (col. 3, lines 1-67, abstract), wherein the security-enabled domain comprises a certificate-based domain (col. 3, lines 36-67).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 2-5.



8. As per claim 6-9, Bathrick does not disclose a method, wherein the certificate-based domain comprises a Kerberos-enabled domain, wherein the matching protocol comprises an X.509 certificate, wherein the security authorization request is generated by the external node, and wherein the step of receiving the security authorization request is executed by the internal node. However, Marino discloses wherein the certificate-based domain comprises a Kerberos-enabled domain, wherein the matching protocol comprises an X.509 certificate (col. 3, lines 36-67), wherein the security authorization request is generated by the external node, and wherein the step of receiving the security authorization request is executed by the internal node (col. 3, lines 1-67, abstract).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 6-9.

9. As per claim 10-12, Bathrick does not disclose a method wherein the security authorization request is generated by the internal node, wherein the step of receiving the security authorization request is executed by the external node, a step of terminating the secure connection when a session between the external node and the internal node is complete. However, Marino discloses wherein the security authorization request is generated by the internal node, wherein the step of receiving the security authorization request is executed by the external node (col. 3, lines 1-67, abstract), a step of terminating the secure connection when a session between the external node and the internal node is complete (col. 4, lines 26-67)

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 10-12.

10. As per claim 13-14, Bathrick disclose a method comprising a step of terminating connection processing when no match between the first protocol set and the second protocol set is found, a step of selecting a protocol to use in establishing the secure connection when a plurality of matching protocols are found (abstract, col. 1, lines 53-67, col. 2, lines 1-32).

11. As per claim 15-16, Bathrick does not disclose a method comprising a step of authenticating at least one of the internal node and the external node, wherein the step of authenticating comprises communicating a certificate to a certificate authority. However, Marino discloses comprising a step of authenticating at least one of the internal node and the external node (col. 3, lines 1-67, abstract), wherein the step of authenticating comprises communicating a certificate to a certificate authority (col. 3, lines 36-67).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 15-16.

12. As per claim 17, Bathrick disclose a system for automatically negotiating a security protocol, a node with an associated first protocol set and a second node having an associated second protocol set, comparing the first protocol set associated with the internal node to the second protocol set associated with the external node, and establishing a secure connection between the external node and the internal node when a matching protocol between the first protocol set and the second protocol set is found

(abstract, col. 1, lines 53-67, col. 2, lines 1-32). He does not expressly disclose an internal node, the internal node being internal to a security-enabled domain and a negotiation engine, the negotiation engine receiving a security authorization request to establish a secure connection between the internal node and [[the]] an external node being external to the security-enabled domain. However, Marino discloses an internal node, the internal node being internal to a security-enabled domain and a negotiation engine; the negotiation engine receiving a security authorization request to establish a secure connection between the internal node and [[the]] an external node being external to the security-enabled domain (col. 3, lines 1-67, abstract).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 17.

13. Claims 18-32 are listed all the same elements of claim 2-16 but in a system form rather than a method form. Therefore, the supporting rationales of the rejection to claim 2-16 apply equally as well to claim 18-32.

14. As per claim 49, Bathrick disclose one or more tangible computer-readable media having computer-executable instructions embodied thereon comprising: comparing a first protocol set associated with the internal node to a second protocol set associated with the external node; and establishing a secure connection between the external node and the internal node when a matching protocol between the first protocol set and the second protocol set is found (abstract, col. 1, lines 53-67, col. 2, lines 1-32). He does not expressly disclose receiving a security authorization request to establish a secure connection between an internal node, the internal node being internal to a

security-enabled domain, and an external node, the external node being external to the security-enabled domain. However, Marino discloses disclose receiving a security authorization request to establish a secure connection between an internal node, the internal node being internal to a security-enabled domain, and an external node, the external node being external to the security-enabled domain (col. 3, lines 1-67, abstract).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 49.

15. Claims 50-62 are listed all the same elements of claim 2-16 but in a computer readable medium form rather than a method form. Therefore, the supporting rationales of the rejection to claim 2-16 apply equally as well to claim 50-62.

### **Conclusion**

**16. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the

Application/Control Number:  
10/608,334  
Art Unit: 2136

Page 12

statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **MOAZZAMI NASSER G** can be reached on **(571)272-4195**. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mohammad Wasim Reza  
AU 2136

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
11/20/07